ISO-IEC-27035-Lead-Incident-Manager Tests & ISO-IEC-27035-Lead-Incident-Manager Prüfungs

Machen Sie sich noch Sorgen um die schwere PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung? Keine Sorgen. Mit den Schulungsunterlagen zur PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung von Fast2test ist jede IT-Zertifizierung einfacher geworden. Die Schulungsunterlagen zur PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung von Fast2test sind der Vorläufer für die PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung.

PECB ISO-IEC-27035-Lead-Incident-Manager Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Fundamental principles and concepts of information security incident management: This section of the exam measures skills of Information Security Analysts and covers the core ideas behind incident management, including understanding what constitutes a security incident, why timely responses matter, and how to identify the early signs of potential threats.
Thema 2	• Improving the incident management processes and activities: This section of the exam measures skills of Incident Response Managers and covers the review and enhancement of existing incident management processes. It involves post-incident reviews, learning from past events, and refining tools, training, and techniques to improve future response efforts.
Thema 3	• Designing and developing an organizational incident management process based on ISO • IEC 27035: This section of the exam measures skills of Information Security Analysts and covers how to tailor the ISO • IEC 27035 framework to the unique needs of an organization, including policy development, role definition, and establishing workflows for handling incidents.
Thema 4	• Information security incident management process based on ISO • IEC 27035: This section of the exam measures skills of Incident Response Managers and covers the standardized steps and processes outlined in ISO • IEC 27035. It emphasizes how organizations should structure their incident response lifecycle from detection to closure in a consistent and effective manner.
Thema 5	• Preparing and executing the incident response plan for information security incidents: This section of the exam measures skills of Incident Response Managers and covers the preparation and activation of incident response plans. It focuses on readiness activities such as team training, resource allocation, and simulation exercises, along with actual response execution when incidents occur.

Das neueste ISO-IEC-27035-Lead-Incident-Manager, nützliche und praktische ISO-IEC-27035-Lead-Incident-Manager pass4sure Trainingsmaterial

Vorm Kauf der Dumps zur ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung von Fast2test können Sie unsere Demo kostenlos als Probe herunterladen.

PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager Prüfungsfragen mit Lösungen (Q22-Q27):

22. Frage
Based on the categorization of information security incidents, incidents such as abuse of rights, denial of actions, and misoperations are categorized as:

- A. Breach of rule incident
- B. Compromise of functions incident
- C. Compromise of information incident

Antwort: A

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1 classifies incidents into several categories based on the nature of their impact. Incidents involving the abuse of user rights, denial of authorized activities, or improper system use are considered violations of internal policies or rules. These fall under the category of "Breach of Rule" incidents.
This category emphasizes that while data or functionality may not be directly compromised, internal governance, permissions, or acceptable use policies have been violated. These incidents are crucial to detect as they often indicate insider threats or misconfigured permissions.
Reference:
ISO/IEC 27035-1:2016, Annex A.2.3: "Breach of Rule" incidents include abuse of privileges, unauthorized activities, and actions violating organizational policies.
Correct answer: C
-

23. Frage
Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.
As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.
In response to the threat detected across its cloud environments. ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation This tool covers network traffic, doud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.
As part of the training initiative. ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack" during the exercise, highlighting the

importance of ongoing education and reinforcement of security awareness principles within the organization.
Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness. ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.
According to scenario 4, in response to a detected threat across its cloud environments, which tool did ORingo utilize to extend its threat detection and response capabilities beyond traditional endpoints?

- A. SIEM
- B. IPS
- C. XDR

Antwort: C

Begründung:
Comprehensive and Detailed Explanation:
XDR (Extended Detection and Response) is a security solution that integrates and correlates data across multiple domains including endpoints, networks, cloud workloads, and more. In the scenario, the tool is described as capable of covering network traffic, cloud environments, and beyond-characteristics that align directly with the capabilities of XDR.
IPS (Intrusion Prevention System) focuses narrowly on network perimeter security.
SIEM (Security Information and Event Management) is primarily focused on log aggregation and analysis rather than real-time detection and automated response across multiple layers.
Reference:
NIST SP 800-207 and modern security frameworks define XDR as a centralized detection and response platform with cross-domain visibility.
Therefore, the correct answer is A: XDR
-

24. Frage
Scenario 6: EastCyber has established itself as a premier cyber security company that offers threat detection, vulnerability assessment, and penetration testing tailored to protect organizations from emerging cyber threats. The company effectively utilizes ISO/IEC 27035-1 and 27035-2 standards, enhancing its capability to manage information security incidents.
EastCyber appointed an information security management team led by Mike. Despite limited resources, Mike and the team implemented advanced monitoring protocols to ensure that every device within the company's purview is under constant surveillance. This monitoring approach is crucial for covering everything thoroughly, enabling the information security and cyber management team to proactively detect and respond to any sign of unauthorized access, modifications, or malicious activity within its systems and networks.
A recent incident involving unauthorized access to company phones highlighted the critical nature of incident management. Nate, the incident coordinator, quickly prepared an exhaustive incident report. His report detailed an analysis of the situation, identifying the problem and its cause. In response to the incident, EastCyber addressed the exploited vulnerabilities. This action started the eradication phase, aimed at systematically eliminating the elements of the incident.
Based on scenario 6, answer the following:
EastCyber decided to address vulnerabilities exploited during an incident as part of the eradication phase, to eradicate the elements of the incident. Is this approach acceptable?

- A. No, vulnerabilities exploited during an incident should be addressed during the containment phase
- B. No, vulnerabilities exploited during an incident should be addressed during the recovery phase
- C. Addressing vulnerabilities exploited during an incident is appropriate during the eradication phase

Antwort: C

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016, the eradication phase of incident management is defined as the stage in which the causes and components of the incident-such as malware, unauthorized access points, or system vulnerabilities-are completely removed or neutralized.
Clause 6.4.5 of ISO/IEC 27035-2 clearly outlines that the eradication phase includes actions to eliminate the root causes of incidents, which may include fixing exploited vulnerabilities and removing malicious code.
This ensures that the underlying issues that allowed the incident to occur are effectively resolved, reducing the risk of recurrence.
While containment aims to limit the damage and prevent the spread of an incident, it is not intended for remediation of vulnerabilities.
Similarly, the recovery phase focuses on restoring services and returning systems to normal operations after the threat has been

eradicated.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 6.4.5: "The eradication phase includes removing the root cause of the incident (e.g., patching vulnerabilities, deleting malware, and closing open ports)." Clause 6.4.3: "Containment is primarily focused on limiting the scope and impact, not resolving root causes." Correct answer: A

25. Frage
Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.
As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.
In response to the threat detected across its cloud environments. ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation This tool covers network traffic, doud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.
As part of the training initiative. ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack" during the exercise, highlighting the importance of ongoing education and reinforcement of security awareness principles within the organization.
Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness. ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.
Based on the scenario above, answer the following question:
After identifying a suspicious state in ORingo's system, a member of the IRT initiated a company-wide system shutdown until the anomaly was investigated. Is this acceptable?

- A. No, the IRT should have determined the facts that enable detection of the event occurrence
- B. Yes, the correct action is to initiate a company-wide system shutdown until the anomaly is investigated
- C. No, the IRT should have immediately informed all employees about the potential data breach

Antwort: A

Begründung:
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-1:2016, particularly in Clause 6.2.2 (Assess and Decide), the organization must first assess the reported event to determine whether it qualifies as a security incident before implementing disruptive responses such as a full system shutdown.
Initiating a shutdown without first determining the cause, impact, or whether it's a confirmed incident can lead to unnecessary operational disruption and loss of services. The proper approach is to collect evidence, analyze system behavior, and make informed decisions based on risk level and confirmed facts.
Option B best reflects the required approach: The IRT should first determine the facts that enable detection and validation of the event's occurrence and impact before initiating drastic action like shutting down critical systems.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.2 - "An analysis should be conducted to determine whether the event should be treated as an information security incident." Clause 6.2.3 - "Response should be proportionate to the impact and type of the incident." Therefore, the correct answer is B.
-

26. Frage

Scenario 8: Moneda Vivo, headquartered in Kuala Lumpur. Malaysia, is a distinguished name in the banking sector. It is renowned for its innovative approach to digital banking and unwavering commitment to information security. Moneda Vivo stands out by offering various banking services designed to meet the needs of its clients. Central to its operations is an information security incident management process that adheres to the recommendations of ISO/IEC 27035-1 and 27035-2.
Recently. Moneda Vivo experienced a phishing attack aimed at its employees Despite the bank's swift identification and containment of the attack, the incident led to temporary service outages and data access issues, underscoring the need for improved resilience The response team compiled a detailed review of the attack, offering valuable insights into the techniques and entry points used and identifying areas for enhancing their preparedness.
Shortly after the attack, the bank strengthened its defense by implementing a continuous review process to ensure its incident management procedures and systems remain effective and appropriate While monitoring the incident management process, a trend became apparent. The mean time between similar incidents decreased after a few occurrences; however, Moneda Vivo strategically ignored the trend and continued with regular operations This decision was rooted in a deep confidence in its existing security measures and incident management protocols, which had proven effective in quick detection and resolution of issues Moneda Vivo's commitment to transparency and continual improvement is exemplified by its utilization of a comprehensive dashboard. This tool provides real time insights into the progress of its information security incident management, helping control operational activities and ensure that processes stay within the targets of productivity, quality, and efficiency. However, securing its digital banking platform proved challenging.
Following a recent upgrade, which included a user interface change to its digital banking platform and a software update, Moneda Vivo recognized the need to immediately review its incident management process for accuracy and completeness. The top management postponed the review due to financial and time constraints.
According to scenario 8, which reporting dashboard did Moneda Vivo use?

- A. Tactical
- B. Strategic
- C. Operational

Antwort: C

Begründung:
Comprehensive and Detailed Explanation From Exact Extract:
The scenario mentions that Moneda Vivo uses a dashboard that offers "real-time insights into the progress of its information security incident management, helping control operational activities and ensure that processes stay within the targets of productivity, quality, and efficiency." These characteristics are aligned with an operational dashboard. According to ISO/IEC 27035-2 and related best practices, operational dashboards track day-to-day activities, monitor KPIs related to incident management, and help frontline teams manage incidents in real time.
Strategic dashboards (Option A) are used by executives for long-term decision-making, while tactical dashboards (Option C) are used for mid-term planning and departmental coordination.
Reference:
ISO/IEC 27035-2:2016, Clause 7.4.6: "Dashboards can support monitoring of incident management activities at operational and tactical levels." Correct answer: B
-

27. Frage
.....

Melden Sie sich an PECB ISO-IEC-27035-Lead-Incident-Manager Zertifizierungsprüfung an? Haben Sie vor zu vielen Prüfungsunterlagen Kopfschmerzen? Wir Fast2test können diese Probleme auflösen und wir sind die Website, an der Sie glauben können. Wenn Sie unsere Unterlagen zur PECB ISO-IEC-27035-Lead-Incident-Manager Prüfung benutzen, können Sie sehr leicht die PECB ISO-IEC-27035-Lead-Incident-Manager Prüfung bestehen. Sie sollen keine Zeit an den Unterlagen verschwenden, die vielleicht keinen Sinn haben. Probieren Sie bitte den Service von Fast2test.

ISO-IEC-27035-Lead-Incident-Manager Prüfungs: https://de.fast2test.com/ISO-IEC-27035-Lead-Incident-Manager-premium-file.html

- ISO-IEC-27035-Lead-Incident-Manager Prüfungen □ ISO-IEC-27035-Lead-Incident-Manager Examsfragen □ ISO-IEC-27035-Lead-Incident-Manager German ❤ □ Sie müssen nur zu [www.zertfragen.com] gehen um nach kostenloser Download von （ ISO-IEC-27035-Lead-Incident-Manager ） zu suchen □ISO-IEC-27035-Lead-Incident-Manager Prüfungsübungen
- ISO-IEC-27035-Lead-Incident-Manager German ↪ ISO-IEC-27035-Lead-Incident-Manager Examengine □ ISO-IEC-27035-Lead-Incident-Manager Prüfungsmaterialien □ Öffnen Sie ▸ www.itzert.com ◂ geben Sie ➽ ISO-IEC-27035-

Lead-Incident-Manager □ ein und erhalten Sie den kostenlosen Download □ISO-IEC-27035-Lead-Incident-Manager Trainingsunterlagen

- ISO-IEC-27035-Lead-Incident-Manager Echte Fragen □ ISO-IEC-27035-Lead-Incident-Manager Musterprüfungsfragen □ ISO-IEC-27035-Lead-Incident-Manager Ausbildungsressourcen □ Suchen Sie einfach auf 《 www.itzert.com 》 nach kostenloser Download von （ ISO-IEC-27035-Lead-Incident-Manager ） □ISO-IEC-27035-Lead-Incident-Manager Examengine
- Neuester und gültiger ISO-IEC-27035-Lead-Incident-Manager Test VCE Motoren-Dumps und ISO-IEC-27035-Lead-Incident-Manager neueste Testfragen für die IT-Prüfungen □ Öffnen Sie die Webseite 《 www.itzert.com 》 und suchen Sie nach kostenloser Download von ➽ ISO-IEC-27035-Lead-Incident-Manager □ □ISO-IEC-27035-Lead-Incident-Manager Examengine
- Zertifizierung der ISO-IEC-27035-Lead-Incident-Manager mit umfassenden Garantien zu bestehen □ Suchen Sie jetzt auf 「 www.itzert.com 」 nach ➽ ISO-IEC-27035-Lead-Incident-Manager □ und laden Sie es kostenlos herunter □ISO-IEC-27035-Lead-Incident-Manager Prüfungsübungen
- ISO-IEC-27035-Lead-Incident-Manager Buch □ ISO-IEC-27035-Lead-Incident-Manager Vorbereitungsfragen □ ISO-IEC-27035-Lead-Incident-Manager Prüfungsmaterialien □ Öffnen Sie die Website 「 www.itzert.com 」 Suchen Sie □ ISO-IEC-27035-Lead-Incident-Manager □ Kostenloser Download □ISO-IEC-27035-Lead-Incident-Manager Prüfungen
- ISO-IEC-27035-Lead-Incident-Manager Praxisprüfung □ ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten □ ISO-IEC-27035-Lead-Incident-Manager Trainingsunterlagen □ Erhalten Sie den kostenlosen Download von ➠ ISO-IEC-27035-Lead-Incident-Manager □ mühelos über ➠ www.deutschpruefung.com □ □ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten
- Wir machen ISO-IEC-27035-Lead-Incident-Manager leichter zu bestehen! □ Suchen Sie einfach auf ▸ www.itzert.com ◂ nach kostenloser Download von " ISO-IEC-27035-Lead-Incident-Manager " □ISO-IEC-27035-Lead-Incident-Manager Prüfungen
- ISO-IEC-27035-Lead-Incident-Manager Dumps Deutsch □ ISO-IEC-27035-Lead-Incident-Manager Fragen Beantworten □ ISO-IEC-27035-Lead-Incident-Manager Examsfragen !! Öffnen Sie die Website ➽ www.deutschpruefung.com □ Suchen Sie 「 ISO-IEC-27035-Lead-Incident-Manager 」 Kostenloser Download □ □ISO-IEC-27035-Lead-Incident-Manager German
- ISO-IEC-27035-Lead-Incident-Manager Schulungsangebot - ISO-IEC-27035-Lead-Incident-Manager Simulationsfragen - ISO-IEC-27035-Lead-Incident-Manager kostenlos downloden □ ▸ www.itzert.com ◂ ist die beste Webseite um den kostenlosen Download von ➥ ISO-IEC-27035-Lead-Incident-Manager □ zu erhalten □ISO-IEC-27035-Lead-Incident-Manager Echte Fragen
- Aktuelle PECB ISO-IEC-27035-Lead-Incident-Manager Prüfung pdf Torrent für ISO-IEC-27035-Lead-Incident-Manager Examen Erfolg prep □ Öffnen Sie 「 www.pass4test.de 」 geben Sie ➠ ISO-IEC-27035-Lead-Incident-Manager □ ein und erhalten Sie den kostenlosen Download □ISO-IEC-27035-Lead-Incident-Manager Schulungsangebot
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes